UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,515	07/06/2001	Michael Freed	NEXSI-01011US0	4141

28863 7590 08/07/2006

SHUMAKER & SIEFFERT, P. A.
8425 SEASONS PARKWAY
SUITE 105
ST. PAUL, MN 55125

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/900,515	FREED ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,11-35 and 37-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,11-35 and 37-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is response to the communication on 24 May 2006.

2. Claims 1-8, 11-35 and 37-53 are pending in the application.

3. Claims 1-8, 11-35 and 37-53 have been rejected.

4. Claims 9, 10 and 36 have been cancelled.

Information Disclosure Statement

5. The examiner has considered the information disclosure statement filed on 24 May 2006.

Response to Arguments

6. Applicant's arguments filed 22 May 2006 have been fully considered but they are not persuasive.

On pages 11 and 12, the applicant argues that none of the components of the Ellis system operates as an intermediate device that supports both a direct mode and a proxy mode as defined by the applicant's claim.

The examiner respectfully disagrees. Ellis discloses a direct mode. The direct mode as taught by Ellis is when the clients are communicating directly without the interference of the "main server". The proxy mode is when communication goes through the main server.

On page 14, the applicant argues that there is no teaching or suggestion in Ellis of an intermediate device located between a client and a server, where the intermediate device operates in a direct mode to decrypt encrypted data packets and forward unencrypted data packets from the intermediate device to the server using a communication session negotiated by the client and the server.

The examiner respectfully disagrees. Ellis discloses forming a session between a client and the agent server. The agent server decrypts the session communication and redirects the decrypted data to its final destination.

On page 14, with respect to claim 2, the applicant argues that Ellis provides no teaching of modifying negotiation data received from a client prior to forwarding the negotiation data to the destination.

The examiner respectfully disagrees. The examiner asserts that the modifying step of the negotiation data would have been the updating of the "network address translation table".

On page 14, with respect to claim 3, the applicant argues that nothing in Ellis suggests modifying a SYN request.

The examiner respectfully disagrees. The examiner asserts that the modification of the SYN requests is the decryption of the requests. The requests are being altered from an encrypted state to a decrypted state.

On page 16, the applicant argues that Ellis fails to describe an intermediate device that forwards decrypted application data to said one of said of plurality of servers using the communications session established between the client and the server, as required by claim 20.

The examiner respectfully disagrees. The examiner respectfully disagrees. Ellis discloses forming a session between a client and the agent server. The agent server decrypts the session communication and redirects the decrypted data to its final destination.

On pages 17 and 18, the applicant argues that Ellis does not describe an acceleration apparatus that support a proxy mode in combination with a direct mode as claimed by the applicants.

The examiner respectfully disagrees. Ellis discloses that packets are spread so that they follow the shortest paths. This is done to accelerate and offload work in the network.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-8, 11, 45-47, 51 and 53 are rejected under 35 U.S.C. 102(e) as being anticipated by Ellis U.S. Patent No. 6,484,257 B1.

As to claim 1, Ellis discloses a method for secure communications between a client and a server, comprising:

managing a communications negotiation between the client and the server through an intermediate device that supports a direct mode and a proxy mode [column 7 line 11 to column 8 line 27];

receiving encrypted data packets from the client with the intermediate device [column 8 line 54 to column 9 line 49];

decrypting each encrypted data packet with the intermediate device [column 8 line 54 to column 9 line 49];

forwarding unencrypted data packets from the intermediate device to the server using a communication session negotiated by the client and the server

when the intermediate device operates in direct mode [column 7 line 11 to column 8 line 27];

forwarding unencrypted data packets from the intermediate device to the server using a communication session negotiated by the server and the intermediate device when the intermediate device operates in proxy mode [column 7 line 11 to column 8 line 27];

receiving data packets from the server [column 8 line 54 to column 9 line 49];

encrypting the data packets from the server [column 8 line 54 to column 9 line 49]; and

forwarding encrypted data packets to the client [column 8 line 54 to column 9 line 49].

As to claim 2, Ellis discloses that the step of managing comprises:

receiving TCP session negotiation data from the client and modifying the negotiation data prior to forwarding the negotiation data to the server to establish the communications session between the client and the server when operating in direct mode [column 8, lines 28-53].

As to claim 3, Ellis discloses modifying a SYN request from the client to the server to alter the packet transmission parameters [column 8, lines 28-53].

As to claim 4, Ellis discloses that the step of modifying includes modifying at least a maximum segment size value of the data packet [column 6, lines 32-56].

As to claim 5, Ellis discloses that the method further includes the steps of negotiating an SSL session with the client [column 2, lines 36-49].

As to claim 6, Ellis discloses that decrypting comprises decrypting SSL encrypted packet data, and wherein encrypting comprises encrypting a data packet with SSL [column 2, lines 36-49].

As to claim 7, Ellis discloses the step of managing comprises receiving with the intermediate device communication negotiation data directed to the server from the client and responding to the negotiation in place of the server when the intermediate device operates in proxy mode [column 7 line 11 to column 8 line 27].

As to claim 8, Ellis discloses negotiating the communications session between the server and the intermediate device as a separate TCP session [column 8, lines 28-53].

As to claim 11, Ellis discloses prior to the step of receiving encrypted data, of negotiating an encrypted data communications session between the intermediate device and the client [column 9 line 51 to column 10 line 11].

As to claim 45, Ellis discloses an secure sockets layer processing acceleration device, comprising:

a client communication engine establishing a secure communications session with a client device via an open network [column 7 line 11 to column 8 line 27];

a server communication engine establishing an open communications session with a server via a secure network [column 7 line 11 to column 8 line 27]; and

an encryption and decryption engine operable on encrypted data packets received via the open communications session and on clear data received via the open communications session [column 8 line 54 to column 9 line 49],

wherein the communication engine supports: (1) a direct mode in which decrypted data packets are forwarded to the servers using a communication session negotiated by the client and the server, and (2) a proxy mode in which the acceleration device responds to the client on behalf of the server and forwards the decrypted data packets to the server using the open communications session established by the acceleration device and the server [column 8 line 54 to column 9 line 49].

As to claim 46, Ellis discloses that when operating in direct mode the communication engine forwards modified communication session data to the server over the communication session between the client device and the server [column 7 line 11 to column 8 line 27].

As to claim 47, Ellis discloses that when operating in proxy mode the communication engine acts as a proxy for a plurality of servers in communication with the SSL acceleration device [column 2, lines 36-49].

As to claims 51 and 53, Ellis discloses automatically switching the intermediate device from the direct mode to the proxy mode upon detection of a communication error associated with the direct mode [column 7 line 11 to column 8 line 27].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 12, 14 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 as applied to claims 1 and 45 above, and further in view of Fujiyama et al U.S. Patent No. 6,052,728.

As to claims 12 and 48, Ellis does not teach that the step of managing comprises maintaining a database of entries on each session of data packets communicated between the client and the server.

Fujiyama et al teaches maintaining a log of entries on each session of data packets communicated between the client and the server [column 14, lines 9-23].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ellis so that there would have been a relay computer that would have maintained a log of entries n each session of data packets communicated between the client and the server.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ellis by the teaching of Fujiyama et al, as described above, because it provides a method to help locate the cause of a problem that occurs during communication [column 1, lines 24-27].

As to claim 14, the Ellis-Fujiyama combination teaches that the entry further includes an initialization vector [Fujiyama et al column 6, lines 56-65].

9. Claims 13 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 and Fujiyama et al U.S. Patent No. 6,052,728 as applied to claim 12 above, and further in view of Bellaton et al U.S. Patent No. 6,473,425 B1.

As to claims 13 and 15, the Ellis-Fujiyama combination teaches that the database includes an entry for a session comprising a session ID [Fujiyama et al column 7, lines58-62].

The Ellis-Fujiyama combination does not teach that the database includes a TCP Sequence number and an SSL session number. The Ellis-Fujiyama combination does not teach that the entry includes an expected ACK.

Bellaton et al teaches entries that include a TCP Sequence number, SSL session number and an expected ACK [column 8 line 53 to column 9 line 20].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Fujiyama combination so that a TCP Sequence number, SSL session number and an expected ACK would have been included in the database entry.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Fujiyama combination by the teaching of Bellaton et al, as described above, because implementing this method and by comparing a new packet to packets already queued for transmission, unnecessary duplicated transmission of a packet can be avoided where packet transmission has been delayed. Avoiding retransmission of

the queued packet avoids aggravating the network congestion [column 5 line 66 to column 6 line 7].

10. Claims 16, 17 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 as applied to claim 1 above, and further in view of Gelman et al U.S. Patent No. 6,415,329 B1.

As to claims 16 and 17, Ellis teaches receiving encrypted data packets, as discussed above for claim 1.

Ellis does not teach that the step of receiving the encrypted data packets includes receiving data packets including encrypted application data spanning multiple packets, and the step of forwarding includes forwarding a portion of the application data contained in an individual encrypted TCP segments to the server without authentication. Ellis does not teach that the step of authenticating the application data on receipt of all packets including the application data.

Gelman et al teaches receiving packets that includes application data spanning multiple packets, and the step of forwarding includes forwarding a portion of the application data contained in an individual TCP segments to the server without authentication [column 9, lines 16-65]. Gelman et al teaches the step of authenticating the application data on receipt of all packets including the application data [column 9, lines 16-65].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ellis so that the step of receiving the encrypted data packets would have included receiving the data packets that fragmented the application data. The step of forwarding would have included forwarding a portion of the application data

contained in the individual fragmented TCP segments to the server without authentication. The application data would have been authenticated on receipt of all the packets including the application data.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ellis by the teaching of Gelman et al, as described above, because fragmenting the packets maintains a low susceptibility to transmission errors and makes it difficult for a third party to intercept the application [column 2, lines 58-63].

As to claim 19, Ellis teaches that the data is buffered for a length sufficient to complete a block cipher used to encrypt the data [column 9 line 51 to column 10 line 11].

11. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 and Gelman et al U.S. Patent No. 6,415,329 B1 as applied to claim 16 above, and further in view of Holtey et al U.S. Patent No. 5,293,424.

As to claim 18, the Ellis-Gelman combination is silent on the data not being buffered during decryption.

Holtey et al teaches data not being buffered during decryption [column 4 line 59 to column 5 line 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Gelman combination so that the data would not have been buffered during decryption.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Gelman combination by the teaching of Holtey et

al, as described above, because buffering is a time consuming process and the buffered data is subject to attack [column 4 line 59 to column 5 line 2].

12. Claims 20-22, 27 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 in view of Maloney et al U.S. Patent No. 6,253,337 B1.

As to claim 20, Ellis discloses a method for secure communications between a client and one of a plurality of servers performed on an intermediary device, comprising:

establishing a communications session between the client and the one of the plurality of servers by receiving negotiation data from the client intended for the server and forwarding the negotiation data in modified form to the server, and receiving negotiation data from the server intended for the client and forwarding the negotiation data to the client to establish the client and the server as terminations for the communications session [column 8 line 54 to column 9 line 49];

establishing a secure communications session between the client and the intermediary device [column 8 line 54 to column 9 line 49];

receiving encrypted application data from the client at the intermediary device by the secure communication session between the intermediary device and the client [column 8 line 54 to column 9 line 49];

decrypting the application data [column 8 line 54 to column 9 line 49]; and

forwarding decrypted application data from the intermediary device to the one of the plurality of servers using the communications session established between the client and the server [column 8 line 54 to column 9 line 49].

Ellis does not teach:

maintaining a database of the secure communications session including information on the session/packet associations.

Maloney et al teaches maintaining a database of the secure communications session including information on the session/packet associations [column 6, lines 33-51].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ellis so that the proxy server would have had a log that maintained records of the secure communications session including information on the session/packet associations.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ellis by the teaching of Maloney et al because without introducing additional traffic on a network, the system produces a virtual picture of network usage and network vulnerabilities. By organizing the inputs of multiple collection tools into visual schematics, Security Administrators become proactive in assessing network weaknesses and in identifying optimum locations for implementing security measures. With the information revealed by the system of the present invention, Security Administrators can identify potential traffic bottlenecks, locate the existence of backdoors, reduce bandwidth usage, develop profiles of users, and pinpoint illicit activity [column 1, lines 57-67].

As to claim 21, Ellis teaches the method further including the steps of:

receiving at the intermediary device application data from the server destined for the client [column 8 line 54 to column 9 line 49];

encrypting the application data at the intermediary device [column 8 line 54 to column 9 line 49]; and

forwarding the application data to the client along the secure communication session established between the intermediary device and the client [column 8 line 54 to column 9 line 49].

As to claim 22, Ellis teaches that the method further includes the step of selecting one of the plurality of servers for each packet in the communications session and mapping all communications intended for the server to the one of the plurality of servers [column 10 line 61 to column 11 line 4].

As to claim 27, the Ellis-Maloney combination teaches that the entry further includes an initialization vector [column 10 line 61 to column 11 line 4].

As to claim 29, Ellis teaches that the step of forwarding includes:

forwarding data which spans over multiple TCP segments and forwarding data which is not authenticated [column 8, lines 28-54].

13. Claims 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 20 above, and further in view of Cohen et al U.S. Patent No. 6,389,462 B1.

As to claim 23, the Ellis-Maloney combination does not teach that forwarding the application to the data comprises receiving packets from the one of the plurality of servers and modifying the source and destination addresses of the packet to forward the packet to the client.

Cohen et al teaches receiving packets from one of the plurality servers and modifying the source and destination addresses of the packet to return the packet to the client [column 9 line 19 to column 10 line 31].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination so that the proxy would have received packets from one of the servers and modified the source and destination addresses of the packet to return the packet to the client.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination by the teaching of Cohen et al, as described above, because address translation by a proxy server reduces latency and minimizes traffic onto and off of the network [column 1, lines 44-58].

As to claim 24, the Ellis-Maloney combination teaches that the step of decrypting application data comprises decrypting data and forwarding the data on to the one of the plurality of servers via a secure network [Ellis column 8 line 54 to column 9 line 49].

As to claim 25, the Ellis-Maloney combination teaches that the step of receiving application data from the one of the plurality of servers, encrypting the data, and forwarding encrypted data to the client [Ellis column 8 line 54 to column 9 line 49].

14. Claims 26 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 20 above, and further in view of Bellaton et al U.S. Patent No. 6,473,425 B1.

As to claims 26 and 28, the Ellis-Maloney combination teaches an entry for a session ID [Maloney column 5 line 63 to column 6 line 32].

The Ellis-Maloney combination does not teach that the database includes an entry for a session comprising a TCP Sequence number and an SSL session number. The Ellis-Maloney combination does not teach that the entry includes an expected ACK.

Bellaton et al teaches entries that include a TCP Sequence number, SSL session number and an expected ACK [column 8 line 53 to column 9 line 20].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination so that a TCP Sequence number, SSL session number and an expected ACK would have been included in the database entry.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination by the teaching of Bellaton et al, as described above, because implementing this method and by comparing a new packet to packets already queued for transmission, unnecessary duplicated transmission of a packet can be

avoided where packet transmission has been delayed. Avoiding retransmission of the queued packet avoids aggravating the network congestion [column 5 line 66 to column 6 line 7].

15. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 20 above, and further in view of Holtey et al U.S. Patent No. 5,293,424.

As to claim 30, the Ellis-Maloney combination does not teach that the data is not buffered during decryption.

Holtey et al teaches data not being buffered during decryption [column 4 line 59 to column 5 line 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination so that the data would not have been buffered during decryption.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination by the teaching of Holtey et al, as described above, because buffering is a time consuming process and the buffered data is subject to attack [column 4 line 59 to column 5 line 2].

16. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 20 above, and further in view of Boeuf U.S. Patent No. 6,009,502.

As to claim 31, the Ellis-Maloney combination does not teach that the data is buffered for a length sufficient to complete a block cipher used to encrypt the data.

Boeuf teaches that data is buffered for a length sufficient to complete a block cipher [column 5, lines 21-67].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination so that the data would have been buffered for a length sufficient to complete a block cipher used to encrypt the data.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination by the teaching of Boeuf, as described above, because it prevents the client from sending data when the server is no longer able to perform normal data storage operations. Such a protocol will operate to limit the amount of client vital data which might be lost [column 2, lines 36-42].

17. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 20 above, and further in view of Weinstein et al U.S. Patent No. 6,094,485.

As to claim 32, the Ellis-Maloney combination does not teach that the step of forwarding includes authenticating the decrypted data after a final segment of a multi-segment encrypted data stream is received.

Weinstein et al teaches verifying the decrypted data after a final segment of a multi-segment encrypted data stream is received [column 8, lines 37-64].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination so that the step of forwarding would have included verifying the decrypted data after a final segment of a multi-segment data stream was received.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination by the teaching of Weinstein et al, as described above, because it validates that none of the segments of data were altered during transmission by a third party.

18. Claims 33-35, 38, 39, 41 and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 in view of Maloney et al U.S. Patent No. 6,253,337 B1.

As to claims 33, 39 and 41, Ellis discloses an acceleration apparatus coupled to a public network and a secure network, communicating with a client via the public network and communicating with one of a plurality of servers via the secure network, comprising:

a network communications interface [column 8 line 54 to column 9 line 49];

at least one processor [column 8 line 54 to column 9 line 49];

programmable dynamic memory [column 8 line 54 to column 9 line 49];

a communications channel coupling the processor, memory and network communications interface [column 8 line 54 to column 9 line 49];

a client/server open communications session manager [column 8 line 54 to column 9 line 49];

a client secure communication session manager [column 8 line 54 to column 9 line 49]; and

a data packet encryption and decryption engine [column 8 line 54 to column 9 line 49],

wherein the acceleration apparatus is adapted to operate in a direct mode and a proxy mode [column 8 line 54 to column 9 line 49],

wherein in the direct mode the acceleration apparatus decrypts data packets received from the client and forwards the decrypted data packets to one of the servers using a communication session negotiated by the client and the server [column 8 line 54 to column 9 line 49],

wherein in the proxy mode the acceleration apparatus responds to the client on behalf of the server and forwards the decrypted data packets to the server using a communication session negotiated by the acceleration device and the server [column 8 line 54 to column 9 line 49].

Ellis does not teach a client/server secure communications session tracking database.

Maloney et al teaches a client/server secure communications session tracking database [column 6, lines 33-51].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ellis so that the proxy would have had a client/server secure communications session tracking database.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ellis by the teaching of Maloney et al because without introducing additional traffic on a network, the system produces a virtual picture of network usage and network vulnerabilities. By organizing the inputs of multiple collection tools into visual schematics, Security Administrators become proactive in assessing network weaknesses and in identifying optimum locations for implementing security measures. With the information revealed by the system of the present invention, Security Administrators can identify potential traffic bottlenecks, locate the existence of backdoors, reduce bandwidth usage, develop profiles of users, and pinpoint illicit activity [column 1, lines 57-67].

As to claim 34, Ellis teaches that in proxy mode the client open communications session manager and secure communication manager enables the apparatus as a TCP and SSL proxy for the server, as discussed above.

As to claim 35, Ellis teaches that in direct mode the communications session managers enable transparent secure and open communication between the client and the server [column 8 line 54 to column 9 line 49].

As to claim 38, Ellis teaches that data packet encryption and decryption engine performs SSL encryption and decryption on data packets transmitted between the client and the at least one server, as discussed above.

As to claim 52, Ellis teaches that the acceleration apparatus automatically switches from the direct mode to the proxy mode upon detection of a communication error associated with the communication session negotiated by the client and the server [column 8 line 54 to column 9 line 49].

19. Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 33 above, and further in view of Harper et al U.S. Patent No. 6,820,215 B2.

As to claim 37, the Ellis-Maloney combination does not teach a load selection manager balancing the routing of multiple open and secure communications sessions between a plurality of clients and a plurality of servers based on current processing levels of the servers.

Harper et al teaches load selection manager balancing the routing of multiple open and secure communications sessions between a plurality of clients and a plurality of servers [column 6, lines 16-29].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination so that there would have been a load selection manager balancing the routing of multiple open and secure communications sessions between a plurality of clients and a plurality of servers.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination by the teaching of Harper et al, as described above, because it allows heavily accessed Web sites to increase capacity, since multiple server machines can be dynamically added while retaining the abstraction of a single entity that appears in the network as a single logical server. In addition, failure of one or more of the server machines in a server cluster need not completely disable the operation of remainder of the server cluster [column 2, lines 18-33].

20. Claim 40 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 33 above, and further in view of Bellaton et al U.S. Patent No. 6,473,425 B1.

As to claim 40, the Ellis-Maloney combination does not teach that the database includes a TCP Sequence number and an SSL session number.

Bellaton et al teaches entries that includs a TCP Sequence number and SSL session number [column 8 line 53 to column 9 line 20].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination so that a TCP Sequence number and SSL session number would have been included in the database entry.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination by the teaching of Bellaton et al, as described above, because implementing this method and by comparing a new packet to packets already queued for transmission, unnecessary duplicated transmission of a packet can be avoided where packet transmission has been delayed. Avoiding retransmission of the queued packet avoids aggravating the network congestion [column 5 line 66 to column 6 line 7].

21. Claim 42 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 33 above, and further in view of Holtey et al U.S. Patent No. 5,293,424.

As to claim 42, the Ellis-Maloney combination is silent on the data not being buffered during decryption.

Holtey et al teaches data not being buffered during decryption [column 4 line 59 to column 5 line 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination so that the data would not have been buffered during decryption.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination by the teaching of Holtey et al, as described above, because buffering is a time consuming process and the buffered data is subject to attack [column 4 line 59 to column 5 line 2].

22. Claim 43 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 33 above, and further in view of Boeuf U.S. Patent No. 6,009,502.

As to claim 43, the Ellis-Maloney combination does not teach that the data is buffered for a length sufficient to complete a block cipher used to encrypt the data.

Boeuf teaches that data is buffered for a length sufficient to complete a block cipher [column 5, lines 21-67].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination so that the data would have been buffered for a length sufficient to complete a block cipher used to encrypt the data.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination by the teaching of Boeuf, as described above, because it prevents the client from sending data when the server is no longer able to perform normal data storage operations. Such a protocol will operate to limit the amount of client vital data which might be lost [column 2, lines 36-42].

23. Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 33 above, and further in view of Weinstein et al U.S. Patent No. 6,094,485.

As to claim 44, the Ellis-Maloney combination does not teach that client/server open communications session manager performs an authentication process that discards at least a portion of the decrypted, unauthenticated packet application data from the client prior to receiving a final segment of the application data and authenticates the decrypted data using only the remaining portion of the application data.

Weinstein et al teaches verifying the decrypted data after a final segment of a multi-segment encrypted data stream is received [column 8, lines 37-64].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination so that the step of

forwarding would have included verifying the decrypted data after a final segment of a multi-segment data stream was received.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ellis-Maloney combination by the teaching of Weinstein et al, as described above, because it validates that none of the segments of data were altered during transmission by a third party.

24. Claim 49 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 as applied to claim 45 above, and further in view of Holtey et al U.S. Patent No. 5,293,424.

As to claim 49, Ellis is silent on the data not being buffered during decryption.

Holtey et al teaches data not being buffered during decryption [column 4 line 59 to column 5 line 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ellis so that the data would not have been buffered during decryption.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ellis by the teaching of Holtey et al, as described above, because buffering is a time consuming process and the buffered data is subject to attack [column 4 line 59 to column 5 line 2].

25. Claim 50 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis U.S. Patent No. 6,484,257 B1 as applied to claim 45 above, and further in view of Harper et al U.S. Patent No. 6,820,215 B2.

As to claim 50, Ellis does not teach a load balancing engine that selects the server from a plurality of servers based on a load balancing algorithm that calculates current processing loads associated with each of the servers.

Harper et al teaches load balancing of servers [column 6, lines 16-29].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ellis so that the servers would have been load balanced.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ellis by the teaching of Harper et al, as described above, because it allows heavily accessed Web sites to increase capacity, since multiple server machines can be dynamically added while retaining the abstraction of a single entity that appears in the network as a single logical server. In addition, failure of one or more of the server machines in a server cluster need not completely disable the operation of remainder of the server cluster [column 2, lines 18-33].

Conclusion

26. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy
August 1, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100